IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

FIRST NAMED INVENTOR	:	Nancy Cam WINGET **Confirmation No.: 3154**
FOR	:	SYSTEM AND METHOD FOR PROVISIONING AND AUTHENTICATING VIA A NETWORK
APPLICATION NO.	:	10/724,995
FILING DATE	:	December 1, 2003
EXAMINER	:	Jeffrey D. Popham
ART UNIT	:	2437
CUSTOMER NO.	:	**23380**

REPLY BRIEF

Mail Stop Appeal Briefs - Patent
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

The Final Office Action in the above-identified application was dated April 10, 2009. Applicant filed a Notice of Appeal on July 10, 2009 and an Appeal Brief on September 4, 2009. Appellants were notified of an Examiner's Answer on December 3, 2009.

The period for responding to the Examiner's Answer ends on February 3, 2010. Accordingly, this Reply Brief is timely filed.

Favorable consideration of the instant Reply Brief is respectfully requested.

ARGUMENTS

Claims 1, 2, 5-10, 15-21, 24, 26, and 27 are pending and under final rejection. Claims 3-4, 11-14, 22-23, and 25 have been canceled. Claims 1, 2, 5-10, 15-21, 24, 26, and 27 are on appeal.

Claims 1, 2, 5, 6, 9, 10, 15-21, 24, 26, and 27 stand rejected under U.S.C. § 103(a) as being obvious in view of the combination of U.S. Patent Application Publication 2004/0268126 to Dogan et al. (*hereinafter*, "Dogan"), U.S. Patent 6,978,298 to Kuehr-McLaren (*hereinafter*, "McLaren"), and Paul Funk, Somin Blak Wilson, "draft-ietf-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAO-TTLS)"; Internet draft PPPEXT Working Group; 30 Nov. 2002, pp. 1-40 (*hereinafter*, "Funk"). Claims 5-10 and 20 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dogan in view of McLaren and Funk, and further in view of Downnard (Downnard, Ian, "Public-Key Cryptography extensions into Kerberos", IEEE December 2002/January 2003, p.30-34) (*hereinafter*, "Downnard").

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). *In re Vaeck*, 947 F.2d 488; 20 USPQ2d 1438 (Fed. Cir. 1991). "All words in a claim must be considered in judging the patentability of that claim against the prior art."

For the reasons previously stated and for reasons that will now be set forth, claims 1, 2, 5 - 10, 15-21, 24, 26, and 27 are not obvious in view of the combination of the art of record.

Some Advantages of the Embodiments

The example embodiments of the present application provide advantages not found in or enabled by the art of record including Dogan alone or in combination with McLaren and/or Funk or in combination with McLaren, Funk, and/or Downnard. The advantages include, among other things, more secure, flexible, and extensible provisioning and authentication protocols between entities via a network. In particular, methods, systems, and devices are provided that decouple: i) the means by which a pre-shared key is established and used to secure communications from ii) the actual process of employing and of using authentication mechanisms to gain access to a network.

For example, as described at paragraph [0069] of the instant application as published:

> one embodiment of the present innovation is directed toward a system and method configured to decouple the means by which a key may be established (e.g. master secret) between a server 110 and a peer 120 to secure communications from the actual process of employing the authentication mechanism to gain access to the network.

Figure 1 of the present application illustrates a network block diagram in accordance with one embodiment wherein the decoupling of the protocol of the system 100 is partitioned into three (3) phases, namely a "Provisioning Phase" 130 which may be used to establish a protected access credential (e.g. PAC), a "Tunnel Establishment Phase" 140 which may be used to achieve an authenticated key agreement for securing communications, and an "Authentication Phase" 150 whereby a secure tunnel may be suitably employed to gain network access through use of a suitable authentication mechanism.

With reference to the example embodiment illustrated in Figure 1 for example, the peer 120 may successfully authenticate itself before the server 110 provisions the peer 120 with the PAC. In this case, the decoupling described above between i) the means by which a pre-shared key is established and used to secure communications and ii) the actual process of employing authentication mechanisms to gain access to a network, adds enhanced flexibility to the network system. As further described at paragraph [0076] of the application as published and with continued reference to the example embodiment shown in Figure 1:

> [i]t will be appreciated that the Provisioning Phase 130 may be initiated solely by the peer 120 in order to alleviate the computational overhead and cost in having to establish a master secret every instance a peer 120 desires to gain access to the network. Additionally, as this in-band provisioning mechanism requires asymmetric cryptography; it will be appreciated that there may be devices for which the computational cost of the Diffie-Hellman key agreement is prohibitive. Thus, by decoupling this phase as a provisioning only conversation which is separate to the network access conversation, such devices may opt to bypass in-band provisioning by enabling out-of-band mechanisms to provision the PAC.

In the above, the "network access communication" is an authentication dialog in accordance with an example embodiment.

This decoupling feature enables flexibility and extensibility in networks as also described at paragraph [0077] of the published application for example, wherein:

> [i]n other words, by decoupling this Provisioning Phase 130 as a provisioning only conversation, the present system and method provides the flexibility and extensibility in allowing both server 110 and peer 120 to utilize other tools or protocols more appropriate for their deployment scenario. For instance, while this present protocol explicitly defines one particular in-band mechanism to achieve a shared secret, it will be appreciated that other means, in-band or out-band may be employed for achieving similar results.

The Claims Include Features Not Disclosed in the Art of Record

Independent claim 1 explicitly recites a method including establishing a first tunnel between a peer and a server, tearing down the first tunnel between the peer and the server, and establishing a subsequent new tunnel between the peer and the server. Thereby, actions within the first tunnel are decoupled from the actions in the subsequent new tunnel. Actions in the subsequent new tunnel include an authentication of a relationship between the peer and the server. These are features not disclosed in the art of record.

In particular, a method is recited for authenticating communication between a first and second party via a network. A first secure tunnel is established between a peer and a server using asymmetric encryption in response to determining that a shared secret does not exist between the peer and the server. The shared secret is received via the first secure tunnel between the peer and the server and the first secure tunnel is then torn down. After the peer has received the shared secret and after tearing down the first secure tunnel, a subsequent new secure tunnel is established between the peer and the server using symmetric encryption and the shared secret. A tunnel key is mutually derived for the subsequent new secure tunnel using symmetric cryptography based on the shared secret in response to establishing the subsequent new secure tunnel. A relationship between the peer and the server is then authenticated within the subsequent secure tunnel. The subsequent new secure tunnel is then cryptographically bound with conversations inside the subsequent new secure tunnel.

Contrary to the Examiner's position in the final Office Action and in the Examiner's Answer, for at least the reasons set forth herein below, neither Dogan nor McLaren or Funk,

alone or in combination, or together with Downnard, teach, suggest or fairly disclose these features and, in particular, they are silent on a decoupling feature in a method of authenticating communication between first and second parties wherein actions within the first tunnel are decoupled from the actions in the subsequent new tunnel. As repeatedly described in the specification including at paragraph [0018] for example, in accordance with one example embodiment, the present systems, methods, and protocols, may be suitably configured to achieve mutual authentication by using a shared secret to establish a tunnel used to protect weaker authentication methods (e.g. user names and passwords). The shared secret, referred to in this embodiment as the protected access credential (PAC) may be advantageously used to mutually authenticate a server and a peer upon securing a tunnel for communication via a network. Thus, an authorization policy may be established and subsequently updated as necessary or desired in accordance with the example embodiments.

Independent claim 17 similarly explicitly recites establishing a first secure tunnel between a peer and a server, tearing down the first secure tunnel between the peer and the server, and establishing a subsequent new secure tunnel between the peer and the server. Thereby, actions within the first tunnel are decoupled from the actions in the subsequent new tunnel. Actions in the subsequent new tunnel include an authentication of a relationship between the peer and the server.

In particular, a system is recited for communicating via a network. A first secure tunnel is established between a peer and a server using asymmetric encryption in response to determining that a shared secret does not exist between the peer and the server. The shared secret is received via the first secure tunnel between the peer and the server and the first secure tunnel is then torn down. A subsequent new secure tunnel is established between the peer and the server using symmetric encryption and the shared secret after tearing down the first secure tunnel and after the peer has received the shared secret. A tunnel key is mutually derived for the subsequent new secure tunnel using symmetric cryptography based on the shared secret in response to establishing the subsequent new secure tunnel. A relationship between the peer and the server is then authenticated within the subsequent secure tunnel. The subsequent new secure tunnel is then cryptographically bound with conversations inside the subsequent new secure tunnel.

Again, contrary to the Examiner's position in the final Office Action and in the Examiner's Answer, for at least the reasons set forth herein below, neither Dogan nor McLaren or Funk, alone or in combination, or together with Downnard, teach, suggest or fairly disclose these features and, in particular, the decoupling feature in a system for communicating via a network between a peer and a server wherein actions within the first tunnel are decoupled from the actions in the subsequent new tunnel. As repeatedly described in the specification including at paragraph [0018] for example, in accordance with one example embodiment, the present systems, methods, and protocols, may be suitably configured to achieve mutual authentication by using a shared secret to establish a tunnel used to protect weaker authentication methods (e.g. user names and passwords). The shared secret (PAC) may be advantageously used to mutually authenticate a server and a peer upon securing a tunnel for communication via a network. Thus, an authorization policy may be established and subsequently updated in accordance with the example embodiments.

Independent claim 24 explicitly recites establishes a first secure tunnel between a wireless device and a server, tearing down the first secure tunnel between the wireless device and the server, and establishes a subsequent new secure tunnel between the wireless device and the server. Thereby, actions within the first tunnel are decoupled from the actions in the subsequent new tunnel. Actions in the subsequent new tunnel include a mutual authentication between the wireless device and the server.

In particular, a wireless device is recited comprising a wireless network adapter for sending and receiving wireless signals with a server. The wireless device establishes a first secure tunnel between a peer and a server using asymmetric encryption in response to determining that a shared secret does not exist between the peer and the server. The wireless device receives the shared secret via the first secure tunnel between the peer and the server and the first secure tunnel is then torn down. The wireless device establishes a subsequent new secure tunnel between the peer and the server using symmetric encryption and the shared secret after tearing down the first secure tunnel and after the peer has received the shared secret. A tunnel key is mutually derived for the subsequent new secure tunnel using symmetric cryptography based on the shared secret in response to establishing the subsequent new secure tunnel. A relationship between the peer and the server is then authenticated within the

subsequent secure tunnel. The wireless device derives keying material that binds the subsequent new secure tunnel with all conversations inside the subsequent new secure tunnel.

Once again, contrary to the Examiner's position in the final Office Action and in the Examiner's Answer, for at least the reasons set forth herein below, neither Dogan nor McLaren or Funk, alone or in combination, or together with Downnard, teach, suggest or fairly disclose these features and, in particular, the decoupling feature in a wireless device including a wireless network adapter for sending and receiving wireless signals with a server wherein actions within the first tunnel are decoupled from the actions in the subsequent new tunnel. As repeatedly described in the specification including at paragraph [0018] for example, in accordance with one example embodiment, the present systems, methods, and protocols, may be suitably configured to achieve mutual authentication by using a shared secret to establish a tunnel used to protect weaker authentication methods (e.g. user names and passwords). The shared secret (PAC) may be advantageously used to mutually authenticate a server and a peer upon securing a tunnel for communication via a network. Thus, an authorization policy may be established and subsequently updated in accordance with the example embodiments.

Dogan Does Not Disclose or Suggest the Decoupling or Authenticating Features

Applicants respectfully submit that Dogan does not teach or suggest the decoupling feature of the claims wherein an authentication is performed in a subsequent new tunnel established after an initial tunnel is torn down. The Examiner conceded on page 5 of the Final Office Action of April 10, 2009 that Dogan does not explicitly disclose tearing down the first secure tunnel. The Examiner took the position however that "it is clear that the registration connection is decoupled from the connections that are later opened, and that the registration connection/tunnel is terminated once the parameters discussed in paragraphs 22-23 are distributed." The Examiner essentially repeated this argument in the Examiner's Answer.

Dogan teaches shared secret generation for symmetric cryptography. A master secret is established between a first communication device and a second communication device (see ¶7). A connection is opened between the first communication device and the second communication device (see ¶7). A connection secret is generated from the master secret and used as symmetric

key during the life of the connection (see ¶7). To the contrary, Dogan teaches establishing the master secret during registration (see ¶23). The registration process is defined to include authentication of a user terminal (see ¶22). Thus, Dogan teaches both establishing a master secret and authenticating the peer using the first secure tunnel. A second tunnel is later opened when a user terminal indicates it needs to send data (¶24). Dogan does not teach or suggest the decoupling of the actions within the first tunnel, namely establishing a shared secret, from the actions within the subsequent new secure tunnel, namely authenticating a relationship between entities such as for example between a peer and a server. As noted above, the use of a shared secret to establish a subsequent new tunnel enables a protection of weaker authentication methods which may be advantageously used to mutually authenticate a server and a peer upon securing a tunnel via a network.

Unlike Dogan, in independent claim 1 for example, after the tearing down of the first secure tunnel, a subsequent new secure tunnel is established between the peer and the server using symmetric encryption and the shared secret from the first secure tunnel and after the peer has received the shared secret. A tunnel key is mutually derived for the subsequent new secure tunnel using symmetric cryptography based on the shared secret responsive to establishing the subsequent. Further, an authenticating of a relationship occurs between the peer and the server within the subsequent new secure tunnel upon mutually deriving the tunnel key for the subsequent new secure tunnel. The method further includes cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel.

The Examiner argues that the entities of Dogan communicating inside the subsequent new secure tunnel by using the connection secret is the same as the conversation being bound to the tunnel. The Examiner also argues such as on page 5 of the Examiner's Answer that paragraphs [0024] - [0026] of Dogan disclose authenticating a relationship between a peer and a server "by the fact that both entities, and only those entities, can generate the connection secret."

Applicants respectfully submit that these arguments are essentially the same and, further, that Dogan therefore fails to teach or suggest, with reference to independent claim 1 for example, "authenticating a relationship between the peer and the server within the subsequent new secure tunnel upon mutually deriving the tunnel key for the subsequent new secure tunnel." As noted above, at least this feature of the claim is lacking in the teachings of Dogan wherein the feature

helps to promote advantages by the embodiments of the present application including the use of the second tunnel and secure communication within the secure tunnel to protect weaker authentication methods (e.g. user names and passwords).

Although in Dogan the tunnel key may be used for secure communication between a peer and a server and that by using the shared tunnel key only the peer and server may communicate, Dogan fails to describe or suggest any authentication within the subsequent new tunnel between the entities. Dogan only describes a simple ability to communicate but not an authentication as explicitly set out in the claims of this Appeal.

Paragraph [0048] of the specification of the instant application, for example describes an example embodiment of an "authentication" wherein:

> "Successful authentication", as used herein, refers to an exchange of EAP messages as a result of which the authenticator decides to allow access by the peer, and the peer decides to use this access. The authenticator's decision typically involves both authentication and authorization aspects; the peer may successfully authenticate to the authenticator but access may be denied by the authenticator due to policy reasons.

Further, paragraph [0069] reiterates the nature of the actions which may be taken in the new secure tunnel decoupled from the initial tunnel wherein:

> briefly describing one embodiment of the present system 100, it provides for a protocol suitably configured to protect the transmission of information in a network (e.g. wired or wireless) thereby potentially preventing session attacks and/or disruption. Specifically, one embodiment of the present innovation is directed toward a system and method configured to decouple the means by which a key may be established (e.g. master secret) between a server 110 and a peer 120 to secure communications from the actual process of employing the authentication mechanism to gain access to the network.

Although in Dogan the tunnel key may be used for secure communication between a peer and a server of a network and that by using the shared tunnel key only the peer and server may communicate, there is no teaching or suggestion of using the tunnel to employ an authentication mechanism to gain access to the network.

Thus, Dogan does not teach, suggest or fairly disclose every element of independent claim 1 as it is void of any description of an authentication in a second secure tunnel after tearing down an initial first tunnel..

Dogan Combined With McLaren and/or Funk Does Not Suggest the Decoupling or Authenticating Features

The aforementioned deficiencies in Dogan are not remedied by any teachings of Kuehr-McLaren. Kuehr-McLaren teaches a method and apparatus for managing session information in a data processing system (Abstract). A request for a secure connection is received (Abstract). The secure connection is established, wherein information used to facilitate the secure connection is generated (Abstract). The information is stored for a selected period of time, wherein the selected period of time is selected to optimize server resources (Abstract). Kuehr-McLaren, however, does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel or of performing an authentication within the new secure tunnel. Kuehr-McLaren is relied on by the Examiner to teach determining whether a shared secret exists between a peer and a server.

The aforementioned deficiencies of Dogan and Kuehr-McLaren are not remedied by the teachings of Funk. Funk teaches using asymmetric encryption for establishing a tunnel. Funk, however, does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel or of performing an authentication within the new secure tunnel and bound within the tunnel. As discussed herein, communicating within a secure tunnel does not detect or prevent man-in-the-middle attacks. Claim 1 remedies this problem by cryptographically binding the conversation within the tunnel the tunnel.

Therefore, for the reasons set forth, neither Dogan, McLaren or Funk, alone or in combination, teach or suggest all of the elements of independent claim 1. Thus, independent claim 1 is not obvious in view of Dogan, McLaren or Funk.

Claims 2, 5-10, 15-16, and 27 depend directly from claim 1 and therefore contain each and every element of claim 1. If an independent claim is nonobvious under 35 U.S.S. § 103, then any claim depending therefrom is nonobvious. *In re Fine,* 837 F.2d 1071, 5 USPQ2d 1956

(Fed. Cir. 1988). Thus, claims 2, 5-10, 15-16 and 27 are not obvious in view of Dogan, McLaren, Funk or Downnard for the reasons already set forth for claim 1.

Claims 17-21

By way of review, independent claim 17 recites a system for communicating via a network. A first secure tunnel is established between a peer and a server using asymmetric encryption in response to determining that a shared secret does not exist between the peer and the server. The shared secret is received via the first secure tunnel between the peer and the server and the first secure tunnel is then torn down. A subsequent new secure tunnel is established between the peer and the server using symmetric encryption and the shared secret after tearing down the first secure tunnel and after the peer has received the shared secret. A tunnel key is mutually derived for the subsequent new secure tunnel using symmetric cryptography based on the shared secret in response to establishing the subsequent new secure tunnel. A relationship between the peer and the server is then authenticated within the subsequent secure tunnel. The subsequent new secure tunnel is then cryptographically bound with conversations inside the subsequent new secure tunnel.

Therefore, for the reasons set forth, neither Dogan, McLaren or Funk, alone or in combination, teach or suggest all of the elements of independent claim 17. Thus, independent claim 17 is not obvious in view of Dogan, McLaren or Funk.

Claims 18-21 depend directly from claim 17 and therefore contain each and every element of claim 17. If an independent claim is nonobvious under 35 U.S.S. § 103, then any claim depending therefrom is nonobvious. *In re Fine,* 837 F.2d 1071, 5 USPQ2d 1956 (Fed. Cir. 1988). Thus, claims 18-21 are not obvious in view of Dogan, McLaren or Funk, or together with Downnard, for the reasons already set forth for claim 17.

Claims 24 and 26

By way of review, independent claim 24 recites a wireless device comprising a wireless network adapter for sending and receiving wireless signals with a server. The wireless device establishes a first secure tunnel between a peer and a server using asymmetric encryption in response to determining that a shared secret does not exist between the peer and the server. The

wireless device receives the shared secret via the first secure tunnel between the peer and the server and the first secure tunnel is then torn down. The wireless device establishes a subsequent new secure tunnel between the peer and the server using symmetric encryption and the shared secret after tearing down the first secure tunnel and after the peer has received the shared secret. A tunnel key is mutually derived for the subsequent new secure tunnel using symmetric cryptography based on the shared secret in response to establishing the subsequent new secure tunnel. A relationship between the peer and the server is then authenticated within the subsequent secure tunnel. The wireless device derives keying material that binds the subsequent new secure tunnel with all conversations inside the subsequent new secure tunnel.

Therefore, for the reasons set forth, neither Dogan, McLaren or Funk, alone or in combination, teach or suggest all of the elements of independent claim 24. Thus, independent claim 24 is not obvious in view of Dogan, McLaren or Funk.

Claim 26 depends directly from claim 24 and therefore contains each and every element of claim 24. If an independent claim is nonobvious under 35 U.S.S. § 103, then any claim depending therefrom is nonobvious. *In re Fine,* 837 F.2d 1071, 5 USPQ2d 1956 (Fed. Cir. 1988). Thus, claim 26 is not obvious in view of Dogan, McLaren or Funk, or together with Downnard, for the reasons already set forth for claim 24.

Conclusion

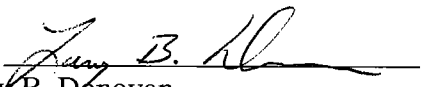
Withdrawal of the rejections to this application is requested for the reasons set forth herein and a Notice of Allowance is earnestly solicited.

If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00010.

Respectfully submitted,

TUCKER ELLIS & WEST LLP

Date: February 2, 2010

By : 

Larry B. Donovan
Registration No. 47,230
Tucker Ellis & West LLP
1150 Huntington Building
925 Euclid Avenue
Cleveland, Ohio 44115-1475
Customer No. 23380
(phone) (216) 696-3864
(fax) (216) 592-5009